

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN**



**BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: THỰC TẬP CƠ SỞ
MÃ HỌC PHẦN: INT13147**

**BÀI THỰC HÀNH 3.4
PHÁT HIỆN LỖ HỒNG VỚI CÔNG CỤ TÌM KIẾM**

Sinh viên thực hiện:

B22DCAT253 Đinh Thị Thanh Tâm

Giảng viên hướng dẫn: TS. Đinh Trường Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

MỤC LỤC.....	2
DANH MỤC CÁC HÌNH VẼ.....	3
DANH MỤC CÁC BẢNG BIỂU	4
CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH.....	5
1.1 Mục đích.....	5
1.2 Tìm hiểu lý thuyết	5
1.2.1 Shodan.....	5
1.2.2 Google Hacking.....	7
CHƯƠNG 2. NỘI DUNG THỰC HÀNH	9
2.1 Các bước thực hiện.....	9
2.1.1 Thử nghiệm với Shodan	9
2.1.2 Thử nghiệm với Google Hacking.....	15
kết luận	28
TÀI LIỆU THAM KHẢO	28

DANH MỤC CÁC HÌNH VẼ

Hình 1 Hướng tiếp cận	6
Hình 2 Ví dụ về kết quả tìm kiếm bằng Google theo cách thông thường	7
Hình 3 Kết quả tìm kiếm bằng Google khi dùng filetype	8
Hình 4 Truy cập vào website shodan	9
Hình 5 Giao diện website shodan sau khi đăng nhập	9
Hình 6 Kết quả sử dụng bộ lọc tìm kiếm các webcam	10
Hình 7 Kết quả sử dụng bộ lọc tìm kiếm các webcam ở Việt Nam	11
Hình 8 Kết quả sử dụng bộ lọc tìm thiết bị sử dụng HTTP trên cổng 8080 tại Việt Nam	11
Hình 9 Kết quả sử dụng bộ lọc tìm FTP server mở	11
Hình 10 Kết quả sử dụng bộ lọc tìm hệ thống router MikroTik tại Việt Nam	12
Hình 11 Kết quả sử dụng bộ lọc tìm hệ thống sử dụng Apache tại PTIT	12
Hình 12 Khởi động Metasploit	13
Hình 13 Công cụ tìm kiếm shodan	13
Hình 14 Xem các tùy chọn có liên quan đến Module	14
Hình 15 Khóa API	14
Hình 16 Thực hiện thiết lập để thực thi module	14
Hình 17 Website Google Hacking	15
Hình 18 Danh mục Filters	15
Hình 19 Trang chi tiết dork	16
Hình 20 Trang chi tiết dork	17
Hình 21 Kết quả tìm kiếm bộ sưu tập được công khai bằng Google	17
Hình 22 Kết quả bộ sưu tập ảnh ngẫu nhiên được công khai	18
Hình 23 Trang chi tiết dork	18
Hình 24 Kết quả tìm kiếm thư mục chứa khóa ssh được công khai bằng Google	19
Hình 25 Kết quả file khóa được công khai ngẫu nhiên	19
Hình 26 Kết quả tìm log có tên người dùng và mật khẩu bằng Google	20
Hình 27 log có tên người dùng và mật khẩu	21
Hình 28 Kết quả tìm kiếm “FTP” bằng Quick Search	21
Hình 29 Kết quả tìm kiếm dork bằng Google	22
Hình 30 Kết quả nhấp vào siêu liên kết	22
Hình 31 Kết quả tìm kiếm dork bằng Google	23
Hình 32 Kết quả nhấp vào siêu liên kết	23
Hình 33 Kết quả tìm kiếm dork bằng Google	24
Hình 34 Kết quả nhấp vào siêu liên kết	24
Hình 35 Kết quả tìm kiếm dork bằng Google	25
Hình 36 Kết quả nhấp vào siêu liên kết	26
Hình 37 Kết quả tìm kiếm dork bằng Google	26
Hình 38 Kết quả nhấp vào siêu liên kết	27

DANH MỤC CÁC BẢNG BIỂU

Bảng 1. Bảng phản hồi từ phía Server.....	6
Bảng 2. Danh sách các bộ lọc thường dùng trong Shodan.....	10
Bảng 3. Giải nghĩa truy vấn intext:"proftpd.conf" "index of"	22
Bảng 4. Giải nghĩa truy vấn inurl: /ftp intitle:"office"	23
Bảng 5. Giải nghĩa truy vấn site:sftp.*./ intext:"login" intitle:"server login"	25
Bảng 6. Giải nghĩa truy vấn "ws_ftp.log" ext:log	26

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1.1 Mục đích

Hiểu được các mối đe dọa đến từ công cụ tìm kiếm như Shodan và Google Hacking, và biết cách khai thác để tìm ra các thông tin nhạy cảm đang bị lộ.

1.2 Tìm hiểu lý thuyết

1.2.1 Shodan

1.2.1.1 Shodan là gì?

Shodan (<https://www.shodan.io/>) là một công cụ tìm kiếm được thiết kế bởi nhà phát triển web John Matherly (<http://twitter.com/achilleian>). Shodan là một công cụ tìm kiếm khác nhiều so với các công cụ tìm kiếm nội dung như Google, Yahoo hoặc Bing.

Không sử dụng cơ chế “cần lướt, sục sạo mạng web để tìm kiếm các website” như Google, Shodan chỉ tập trung thăm dò các kênh sau của mạng Internet. Nói cách khác, nó giống như một Google “đen tối”, chuyên cần quét máy chủ, webcam, máy in, routers và tất cả những thứ khác, miễn là chúng có kết nối với mạng Internet.

Shodan hoạt động 24/7 và thu thập thông tin từ khoảng 500 triệu thiết bị, dịch vụ mỗi tháng.

Bạn sẽ thực sự ngỡ ngàng với những gì mình tìm thấy sau khi thực hiện một thao tác tìm kiếm đơn giản trên Shodan. Vô số đèn giao thông, camera an ninh, các thiết bị tự động trong nhà hay các hệ thống sưởi nhiệt thông minh đều kết nối với Internet và có thể dễ dàng định vị giống như bóc kẹo.

Sau một thời gian dùng quen, bạn có thể tìm thấy hệ thống điều khiển của cả một công viên nước, một trạm xăng, dàn tủ ướp lạnh rượu vang của khách sạn. Các nhà nghiên cứu bảo mật thậm chí còn có thể định vị hệ thống điều khiển và kiểm soát nhà mạng điện hạt nhân hay các lò gia tốc hạt thông qua Shodan.

Điều thực sự đáng nói về khả năng tìm kiếm thông tin của Shodan – cũng như tác nhân khiến cho nó trở nên thực sự đáng sợ – là rất hiếm những thiết bị mà Shodan có thể sục sạo được trang bị các hàng rào bảo mật. “Bạn có thể đăng nhập vào khoảng một nửa mạng Internet với mật khẩu mặc định”, ông HD Moore, Giám đốc Bảo mật của Rapid 7 bình luận. “Đó là một sự thất bại kinh hoàng nhưng chưa được thừa nhận của giới bảo mật”.

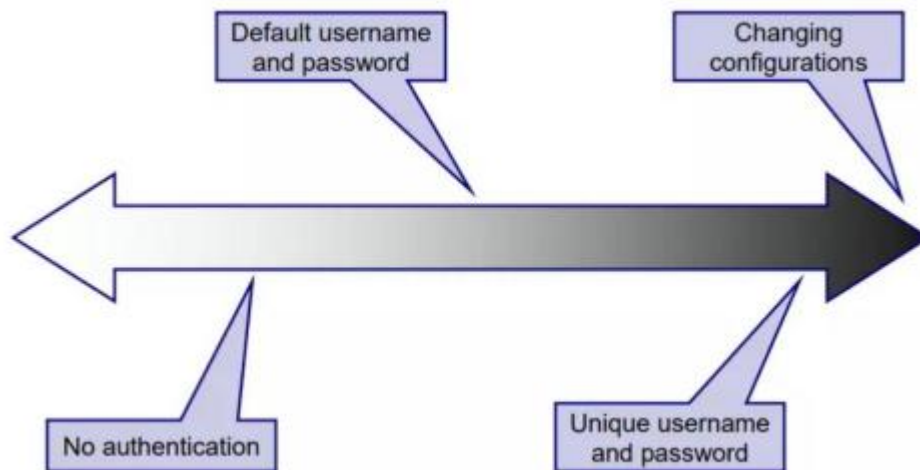
Chỉ một từ khóa tìm kiếm “mật khẩu mặc định” sẽ tiết lộ vô số các thiết bị điều khiển hệ thống, máy in, máy chủ dùng “admin” làm username và “1234” làm mật khẩu chính. Nhiều hệ thống nối mạng thậm chí còn chả có mật khẩu – tất cả những gì bạn cần là một trình duyệt web để có thể kết nối chúng.

1.2.1.2 Ứng dụng shodan trong kiểm thử bảo mật

Pen Testing: Ethics

- Sử dụng shodan để xem hoặc thay đổi cấu hình các thiết bị hay server mà không yêu cầu xác thực

- Sử dụng shodan để xem hoặc thay đổi cấu hình các thiết bị hay server sử dụng tài khoản và mật khẩu mặc định
- Sử dụng shodan để xem hoặc thay đổi cấu hình của các thiết bị sử dụng chung tài khoản mật khẩu
- Sử dụng shodan để xem hoặc thay đổi cấu hình của các thiết bị bị lộ tài khoản và mật khẩu (trong cấu hình hoặc file...)



Hình 1 Hướng tiếp cận

Pen Testing Applications

- Tìm kiếm để kiểm tra xâm nhập các ứng dụng trên thiết bị hay server sử dụng các yếu tố
 - Mã code HTTP trả về
 - Các thông tin banner, foot printing của dịch vụ
 - Phiên bản của dịch vụ
 - Các cổng dịch vụ đang mở

Pen Testing - HTTP Status Codes: Tìm kiếm dựa theo phản hồi từ phía server

Status Code	Description
200 OK	Request succeeded
401 Unauthorized	Request requires authentication
403 Forbidden	Request is denied regardless of authentication

Bảng 1. Bảng phản hồi từ phía Server

1.2.2 Google Hacking

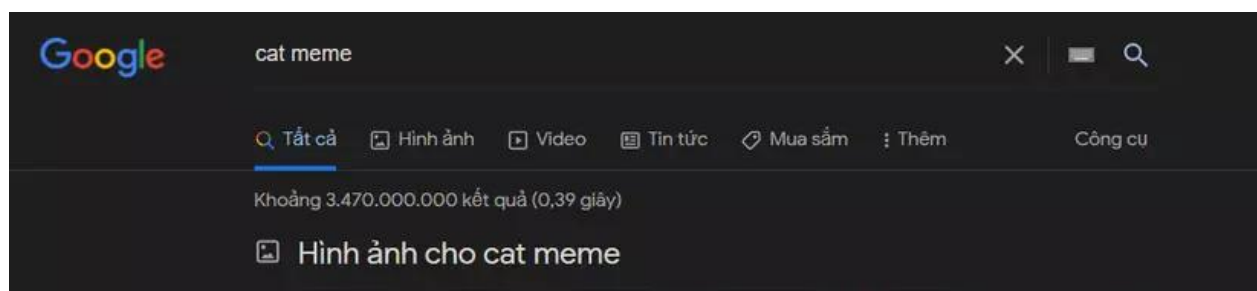
1.2.2.1 Google Hacking là gì?

- Google Hacking Database (GHDB): Đây là một cơ sở dữ liệu chứa các chuỗi truy vấn (dorks) được sử dụng để tìm kiếm các lỗ hổng bảo mật trên các trang web sử dụng Google. GHDB cung cấp các dorks đã được phân loại và được cập nhật Bài 14: Phát hiện lỗ hổng với công cụ tìm kiếm thường xuyên, giúp người dùng tìm kiếm và khám phá các lỗ hổng bảo mật trên trang web một cách hiệu quả.
- Google Dorks: Google Dorks là các chuỗi truy vấn đặc biệt được sử dụng để tìm kiếm thông tin cụ thể trên Google. Bằng cách sử dụng Google Dorks, người dùng có thể tìm kiếm các tài liệu, thông tin bảo mật, thông tin người dùng, tệp đính kèm và nhiều nội dung khác mà không thể tìm thấy thông qua việc tìm kiếm thông thường.
- Google Advanced Search: Google Advanced Search là tính năng đặc biệt của Google cho phép người dùng tìm kiếm chính xác và rõ ràng hơn bằng cách sử dụng các tiêu chí tìm kiếm nâng cao. Với Google Advanced Search, người dùng có thể tìm kiếm đoạn văn bản cụ thể, loại tệp tin, ngôn ngữ, thời gian và vị trí, giúp lọc kết quả tìm kiếm theo yêu cầu cụ thể.
- Google Alerts: Google Alerts là dịch vụ của Google cho phép người dùng theo dõi các từ khóa, cụm từ hoặc tên thương hiệu trên mạng. Khi có thông tin mới liên quan đến từ khóa được theo dõi xuất hiện trên trang web, tin tức hoặc diễn đàn, người dùng sẽ nhận được thông báo qua email. Điều này giúp người dùng duy trì sự cập nhật với các tin tức và thông tin mới nhất về từ khóa quan tâm

1.2.2.2 Các toán tử nâng cao của Google

Nếu ta muốn thực hiện Google Hacking, ta sẽ phải sử dụng các toán tử nâng cao của công cụ tìm kiếm Google. Mục tiêu của nó là tìm các chuỗi văn bản cụ thể trong các kết quả mà tìm kiếm cung cấp cho chúng ta. Các truy vấn mà ta thực hiện trong Google sẽ phụ trách việc tìm kiếm tất cả các trang web thông qua một loại bộ lọc sẽ là toán tử.

Bây giờ, điều đầu tiên chúng ta sẽ làm là mở trình duyệt và truy cập trang web nơi đặt công cụ tìm kiếm của Google. Bước tiếp theo tìm kiếm một từ khóa bất kỳ trên Google, ví dụ như: cat meme



Hình 2 Ví dụ về kết quả tìm kiếm bằng Google theo cách thông thường

Như kết quả tìm kiếm đã thấy, tìm kiếm cho ra gần 3,5 tỷ kết quả. Điều này đôi khi dư thừa thông tin, dẫn đến bão hòa. Bây giờ chúng ta hãy thêm tiêu đề và loại file cần tìm kiếm.

Trong trường hợp này, ta sẽ phải thực hiện tìm kiếm bằng cách nhập intitle: cat meme filetype: pdf



Hình 3 Kết quả tìm kiếm bằng Google khi dùng filetype

Kết quả tìm kiếm được rút gọn đi đáng kể, từ hơn 3B xuống còn 100k kết quả, mặc dù cùng từ khóa tìm kiếm.

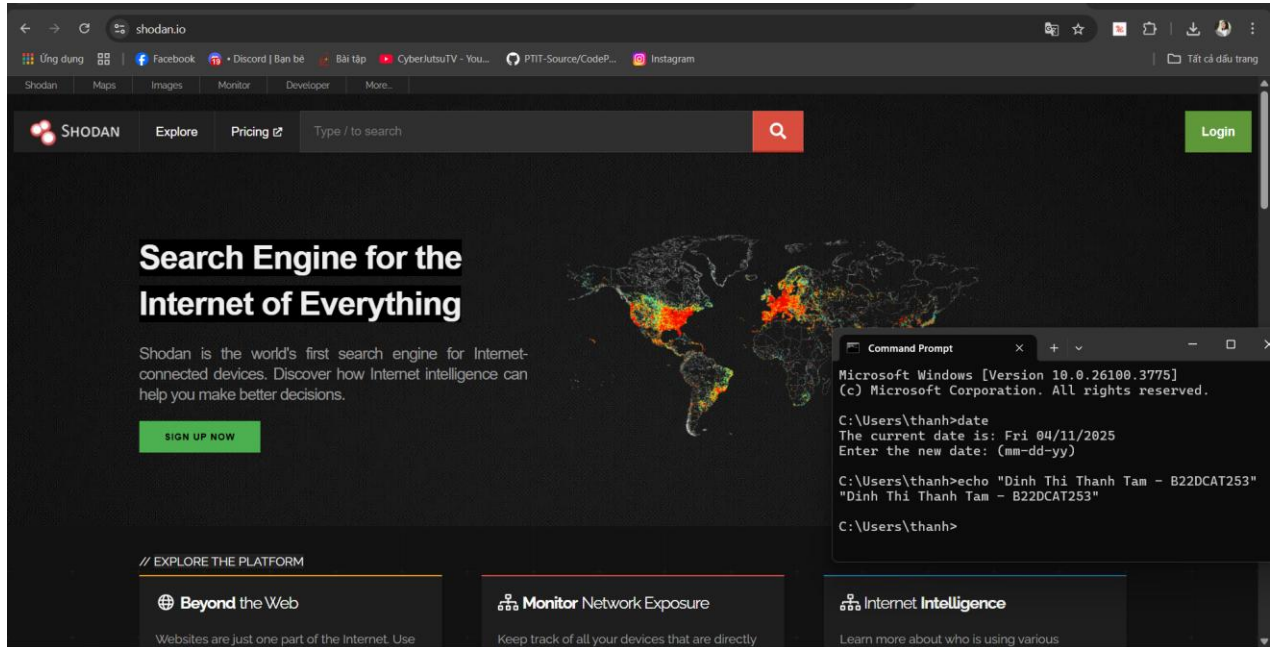
Đối với “filetype”, nó rất dễ sử dụng nếu bạn đã quen và biết các phần mở rộng của tệp. Vì vậy, ví dụ, đối với Word (doc, docx), Excel (xls, xlsx), các trang Web (html, htm), tài liệu văn bản (txt), âm thanh MP3 (mp3) và video AVI

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

2.1 Các bước thực hiện

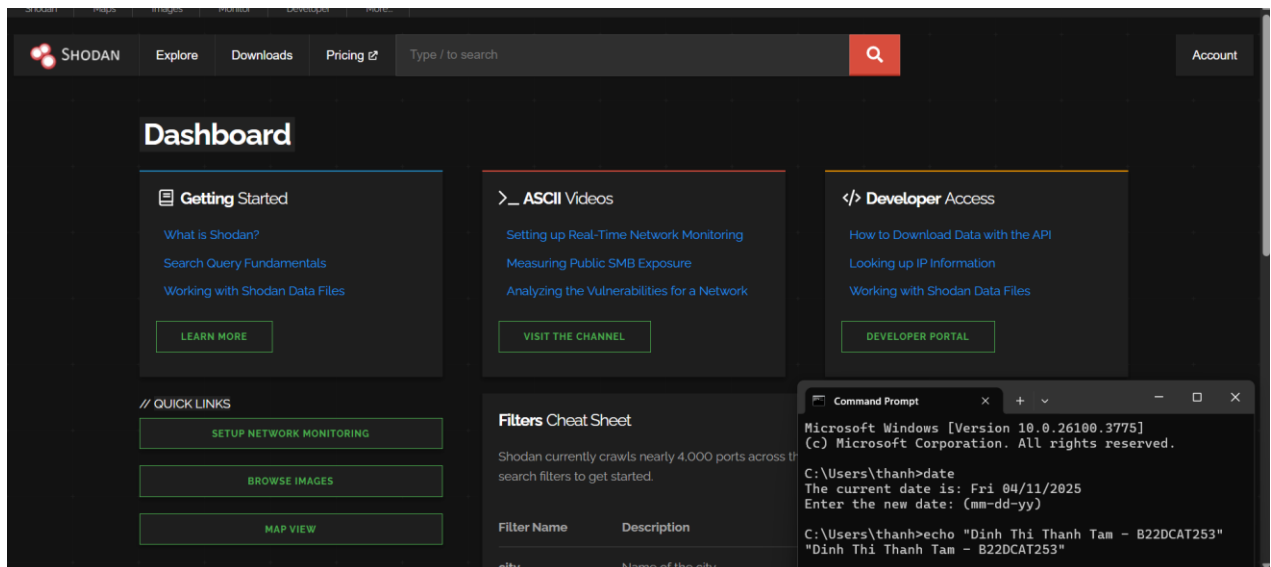
2.1.1 Thử nghiệm với Shodan

- Truy cập trang: <https://www.shodan.io> để vào website shodan



Hình 4 Truy cập vào website shodan

- Tạo tài khoản, đăng nhập sử dụng



Hình 5 Giao diện website shodan sau khi đăng nhập

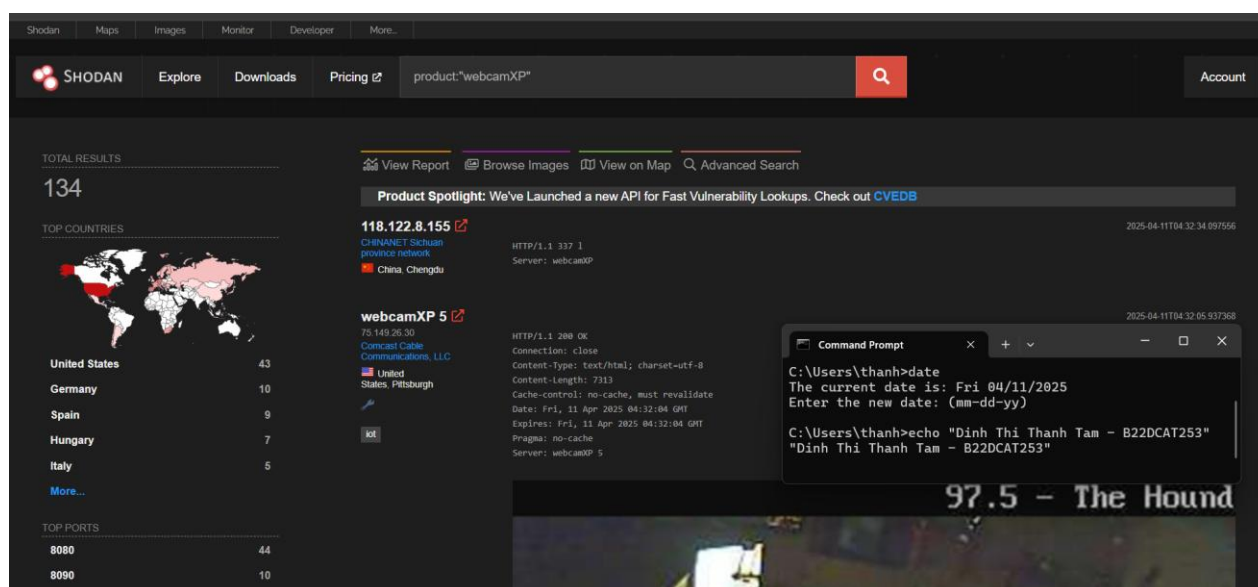
2.1.1.1 Thử nghiệm tìm kiếm bằng bộ lọc

Bộ lọc	Chức năng	Ví dụ sử dụng
country	Lọc theo quốc gia	country:"VN" (Việt Nam)
port	Lọc theo cổng dịch vụ	port:21 (tìm dịch vụ FTP)
org	Lọc theo tổ chức	org:"VNPT"
hostname	Lọc theo tên miền	hostname:"ptit.edu.vn"
net	Lọc theo dải IP	net:"192.168.1.0/24"
os	Lọc theo hệ điều hành	os:Windows 7"
product	Lọc theo tên phần mềm/dịch vụ	product:"Apache"
version	Lọc theo phiên bản dịch vụ	product:"Apache" version:"2.4.7"
before/after	Lọc theo thời gian ghi nhận	before:"2023-01-01"
city	Lọc theo thành phố	city:"Hanoi"
isp	Lọc theo nhà cung cấp dịch vụ internet	isp:"FTP Telecom"

Bảng 2. Danh sách các bộ lọc thường dùng trong Shodan

- Tìm webcam đang mở:

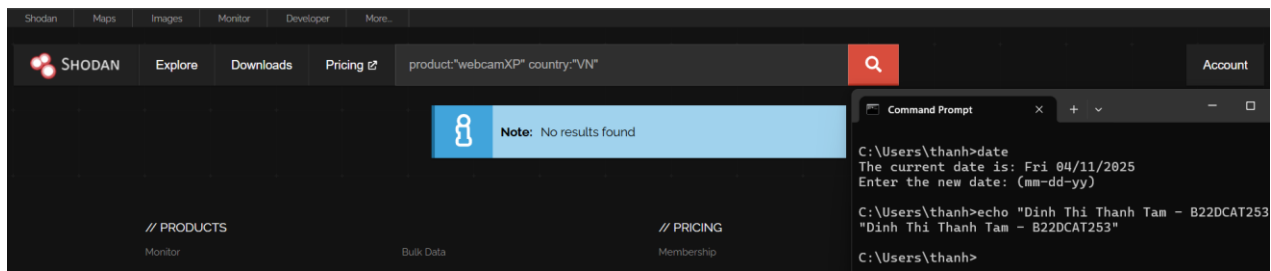
product:"webcamXP"



Hình 6 Kết quả sử dụng bộ lọc tìm kiếm các webcam

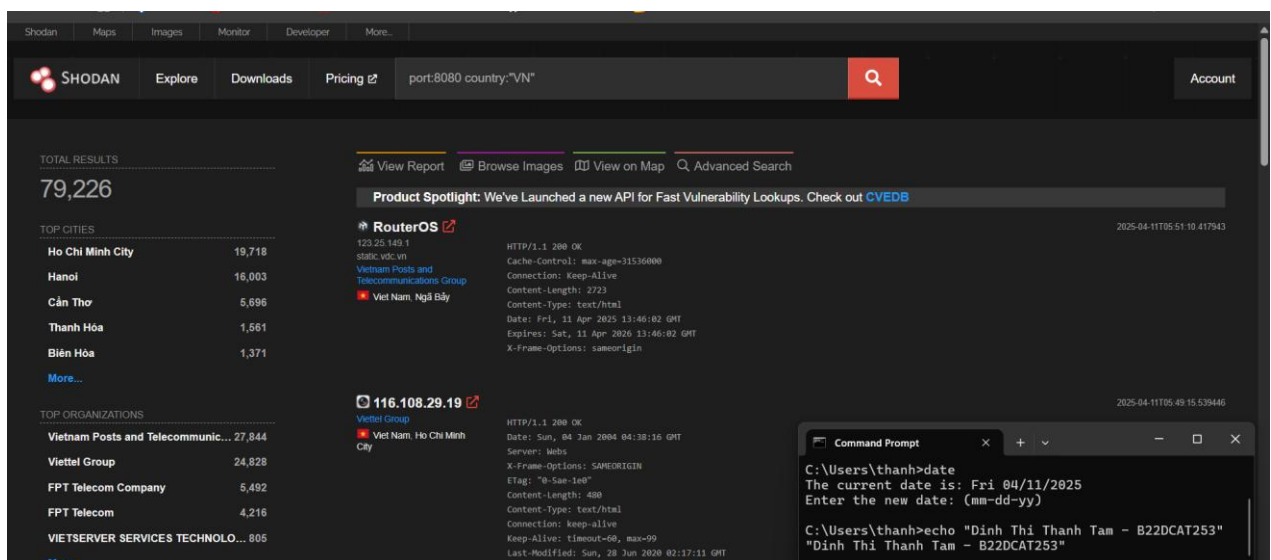
- Tìm webcam ở Việt Nam

product:"webcamXP" country:"VN"



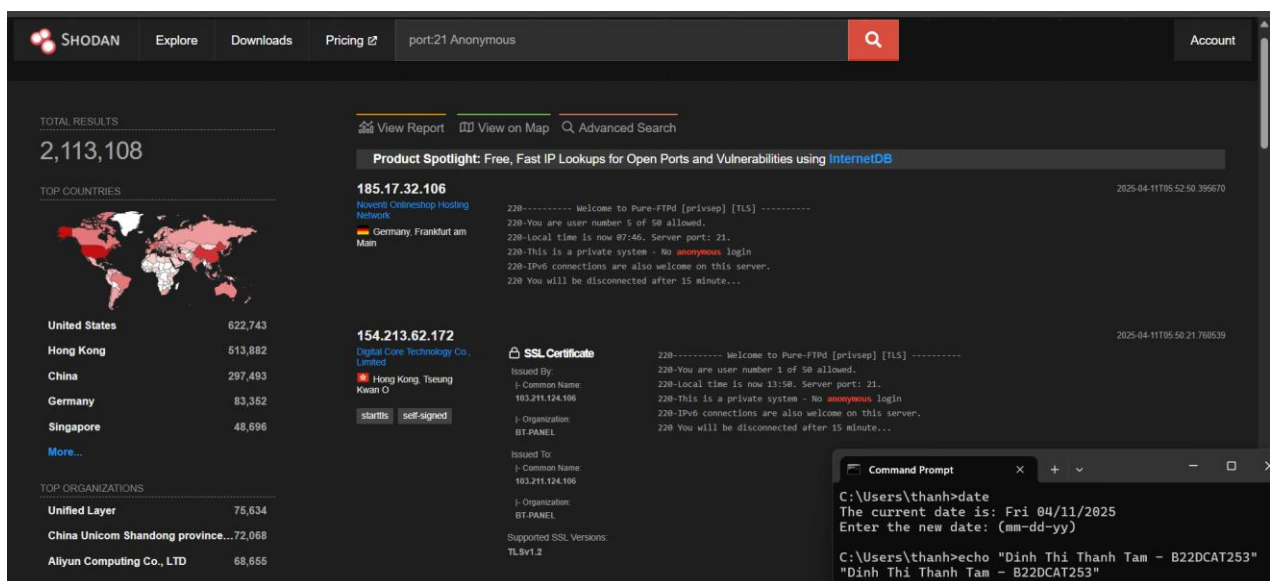
Hình 7 Kết quả sử dụng bộ lọc tìm kiếm các webcam ở Việt Nam

- Tìm thiết bị sử dụng HTTP trên cổng 8080 tại Việt Nam:
port:8080 country:"VN"



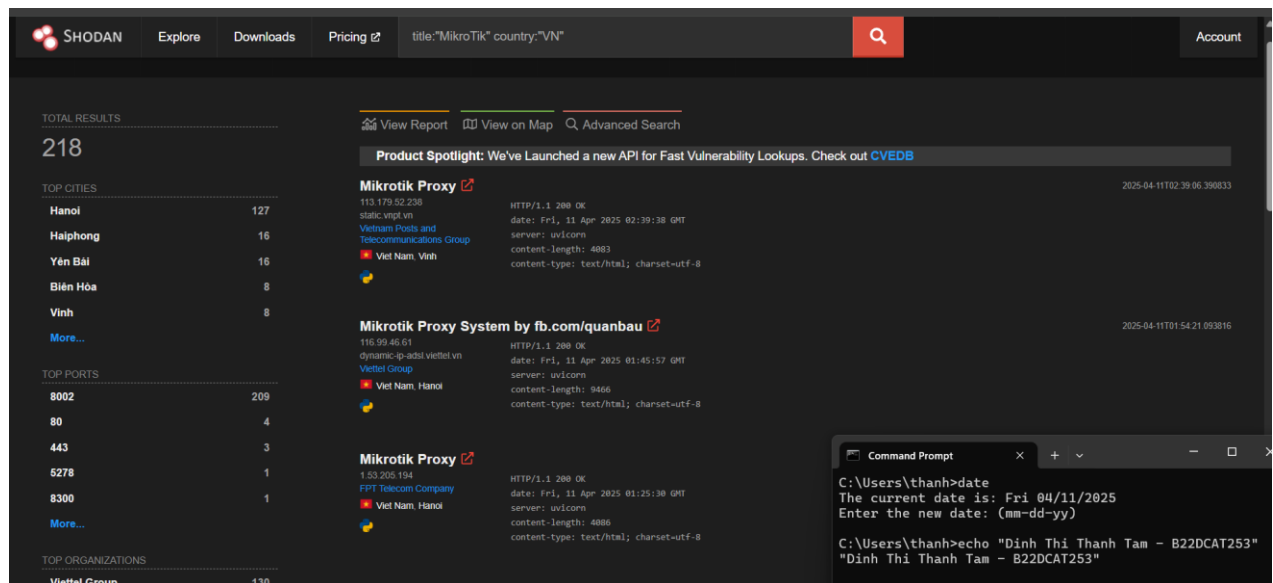
Hình 8 Kết quả sử dụng bộ lọc tìm thiết bị sử dụng HTTP trên cổng 8080 tại Việt Nam

- Tìm FTP server mở
port:21 Anonymous



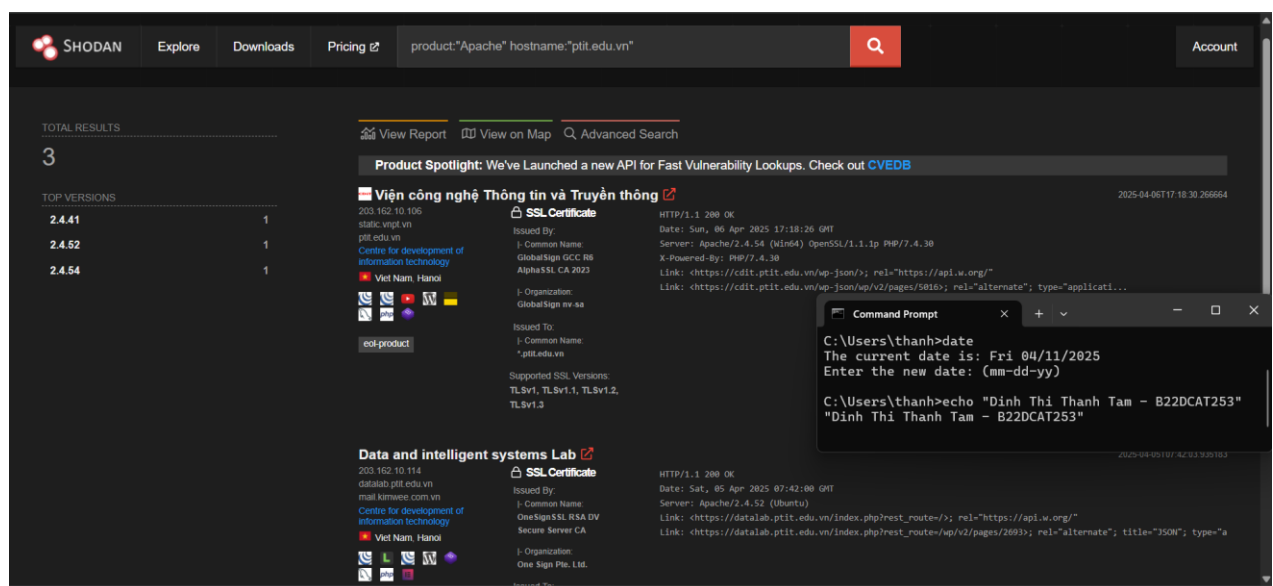
Hình 9 Kết quả sử dụng bộ lọc tìm FTP server mở

- Tìm hệ thống router MikroTik
title:"MikroTik" country:"VN"



Hình 10 Kết quả sử dụng bộ lọc tìm hệ thống router MikroTik tại Việt Nam

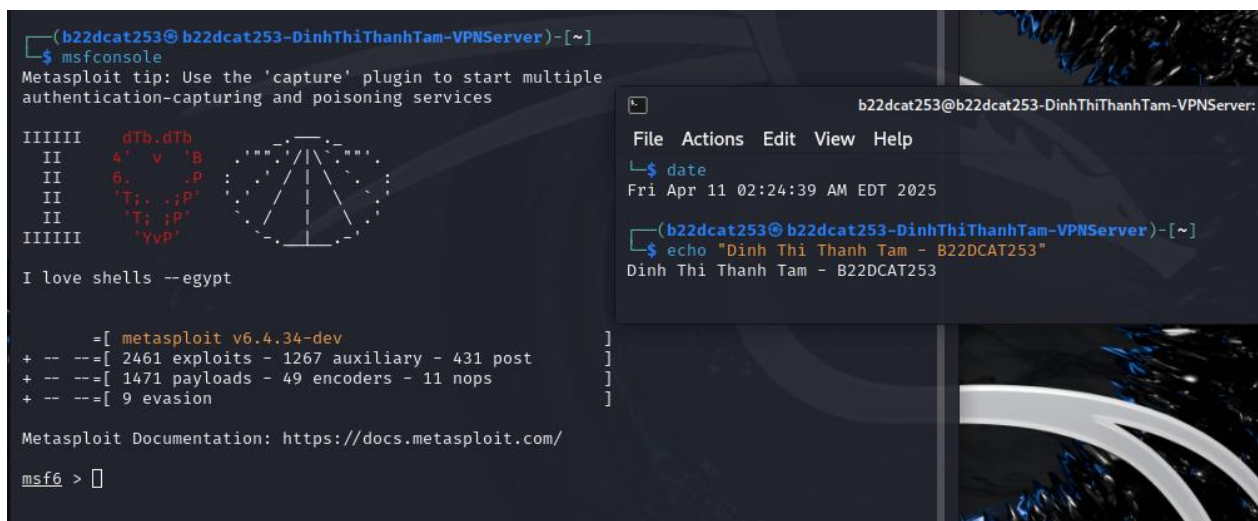
- Tìm hệ thống sử dụng Apache tại PTIT
product:"Apache" hostname:"ptit.edu.vn"



Hình 11 Kết quả sử dụng bộ lọc tìm hệ thống sử dụng Apache tại PTIT

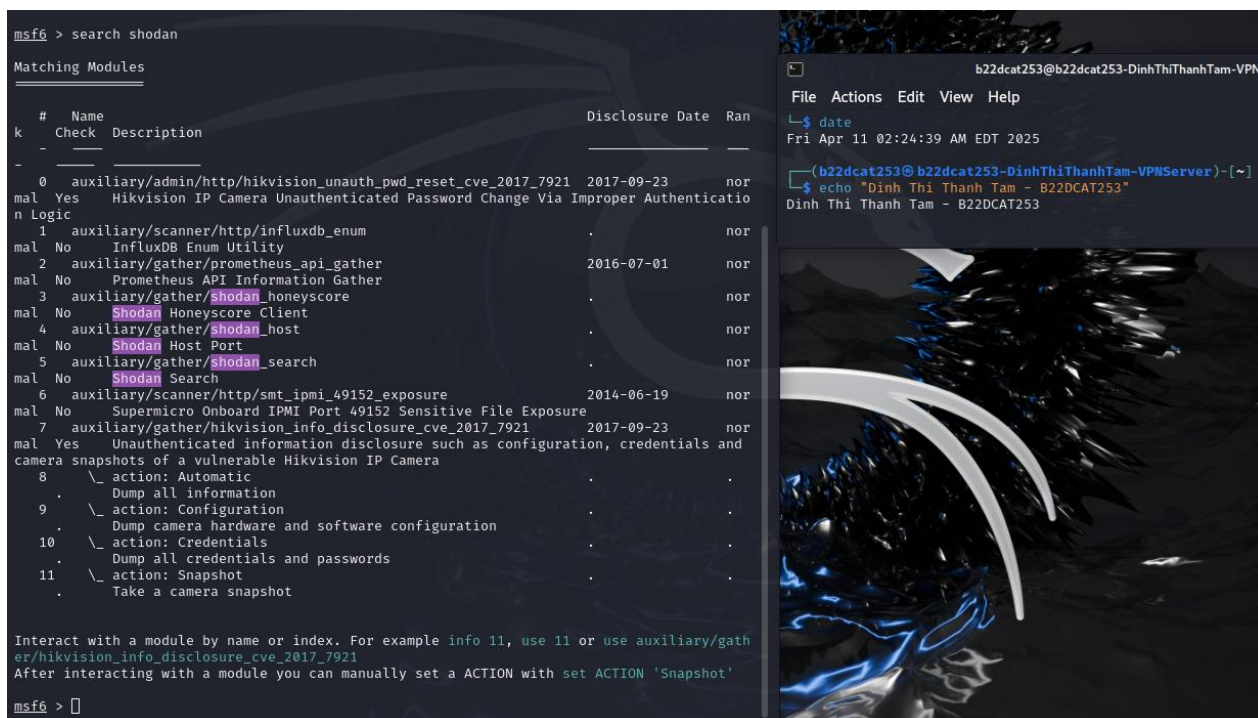
2.1.1.2 Tìm Webcam dễ bị tấn công bằng Shodan [Metasploit Framework]

- Để khởi động Metasploit Framework, hãy nhập “ msfconsole ” từ terminal.



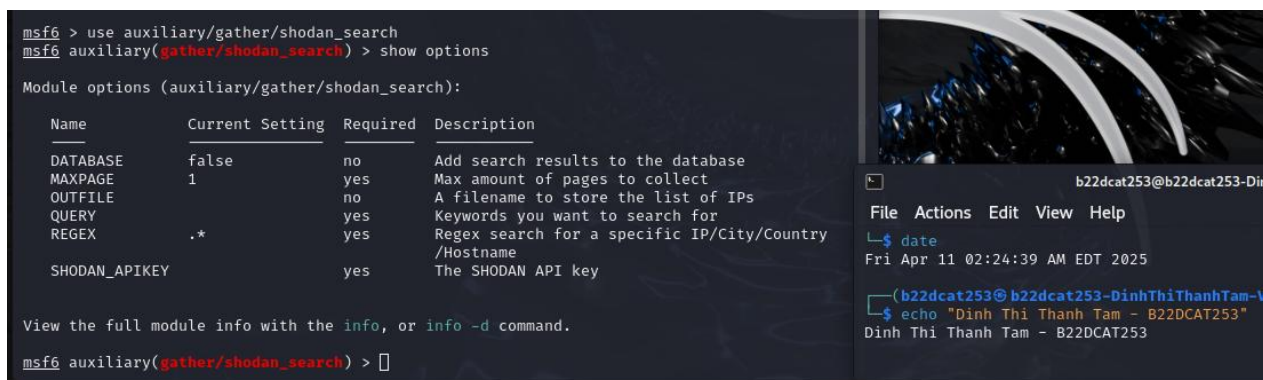
Hình 12 Khởi động Metasploit

- Nhập “ search shodan ” để xem tất cả các mô-đun/lỗ hổng có sẵn liên quan đến công cụ tìm kiếm shodan.



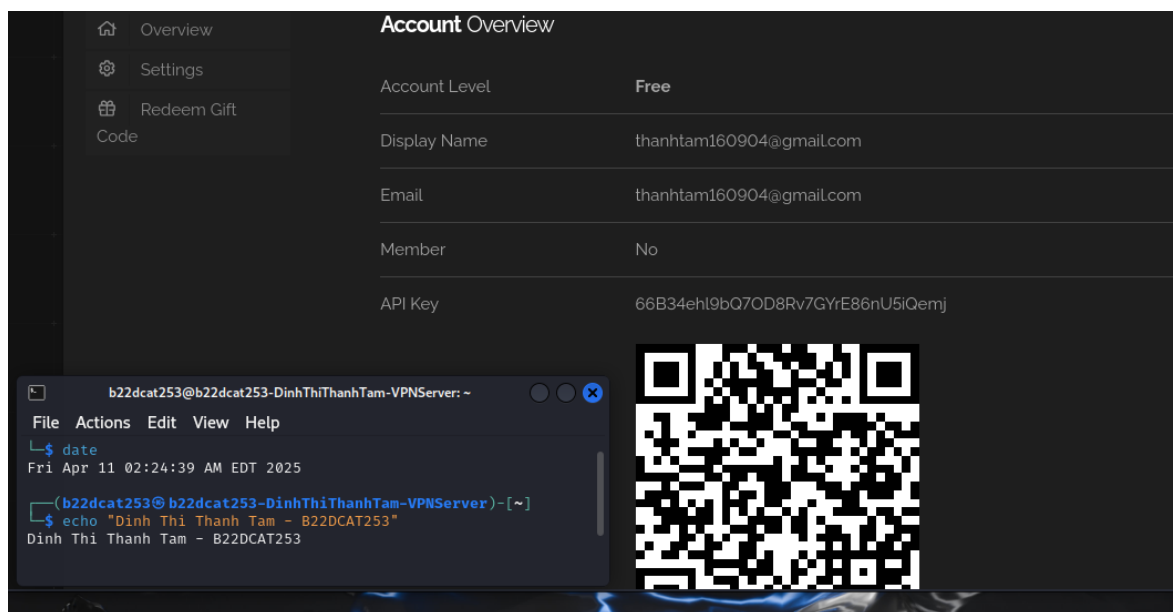
Hình 13 Công cụ tìm kiếm shodan

- Từ tất cả các kết quả trên, chỉ cần nhập “ use auxiliary/gather/shodan_search ”
- Module này sử dụng API Shodan để tìm kiếm Shodan. Đầu ra từ module được hiển thị trên màn hình và có thể được lưu vào tệp hoặc cơ sở dữ liệu MSF. Nhập “show options” cho tất cả các tùy chọn bắt buộc liên quan đến module trên



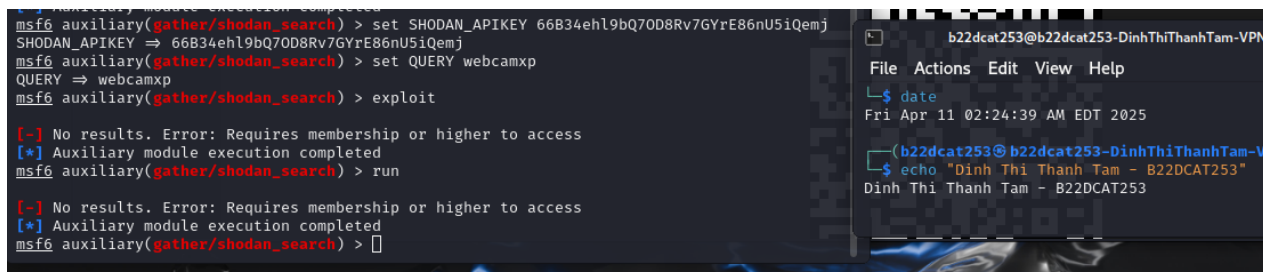
Hình 14 Xem các tùy chọn có liên quan đến Module

- Lấy khóa API từ trang website shodan



Hình 15 Khóa API

- Để thiết lập Khóa Shodan, hãy nhập “ set SHODAN_APIKEY <Khóa API tại đây> ” và thiết lập Truy vấn mà muốn tìm kiếm.
- Trong trường hợp này, tìm kiếm các Webcam dễ bị tấn công, vì vậy nhập “ set QUERY webcamxp ”, thực thi mô-đun bằng cách nhập run hoặc exploit từ bảng điều khiển msf.



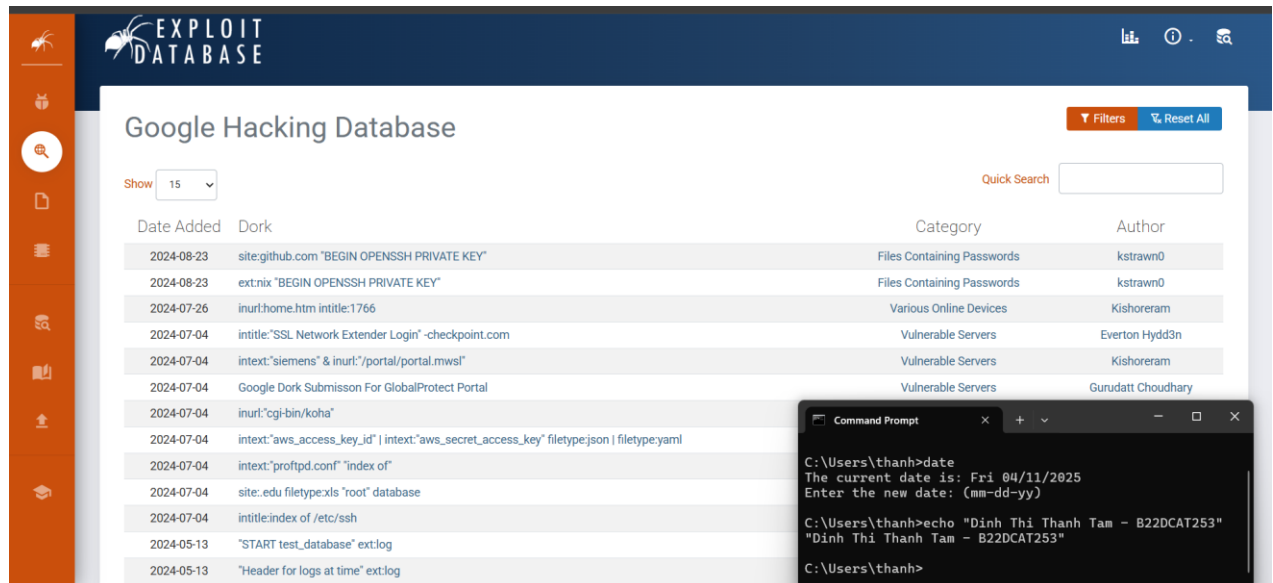
Hình 16 Thực hiện thiết lập để thực thi module

- Ngay sau khi chạy mô-đun thành công sẽ nhận được tất cả kết quả hiển thị tất cả các camera web mở dễ bị tấn công được lưu trữ ở nhiều vị trí khác nhau.

2.1.2 Thử nghiệm với Google Hacking

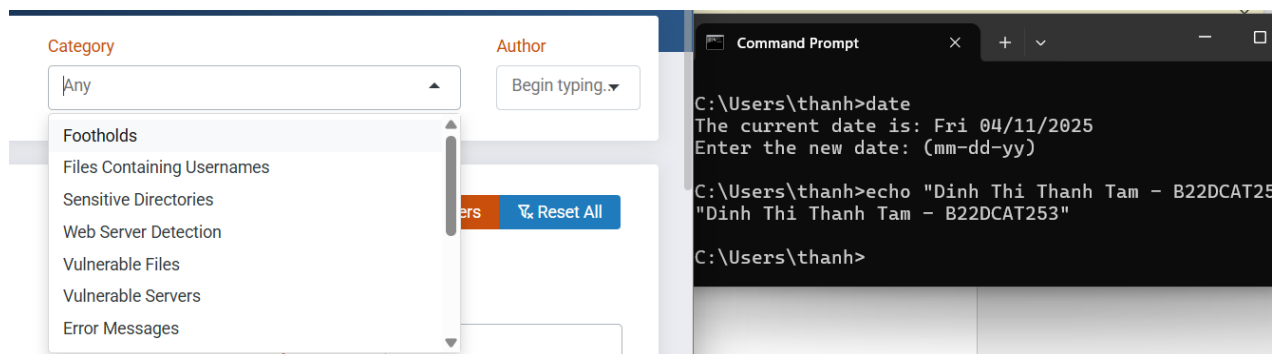
2.1.2.1 Truy cập GHDB

- Vào trang: <https://www.exploit-db.com/google-hacking-database>



Hình 17 Website Google Hacking

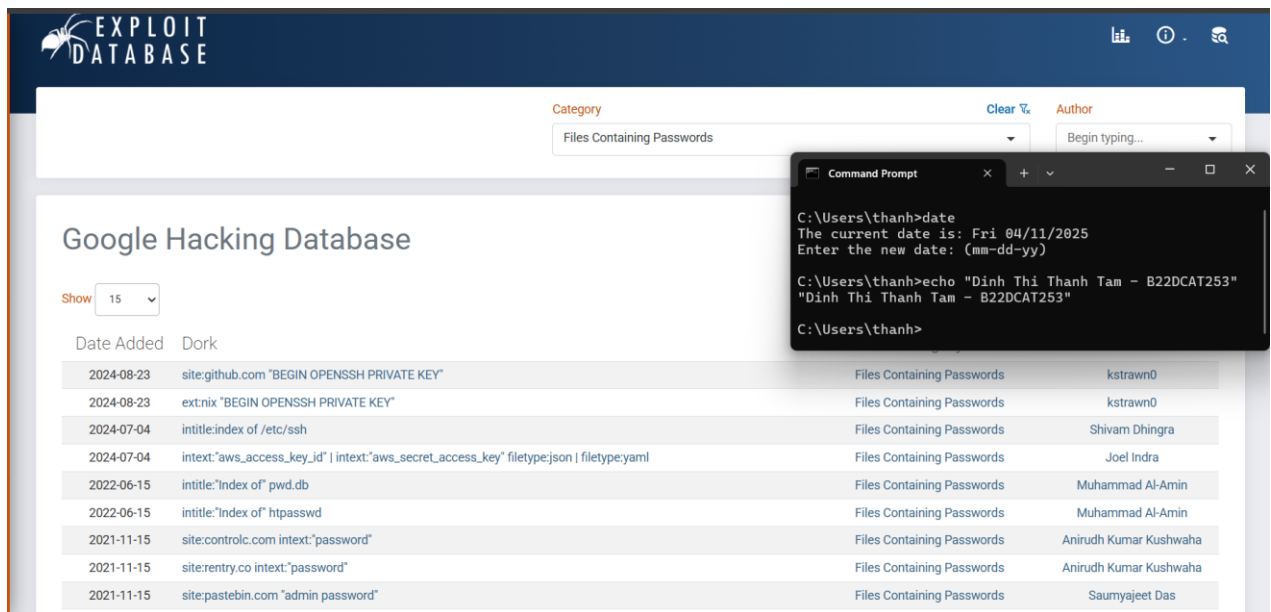
- Nhấn nút “Filters” (góc trên bên phải)
- Dùng menu xổ xuống để xem các danh mục như:
 - Footholds
 - Files Containing Passwords
 - Sensitive Directories
 - Web Server Detection
 - etc.



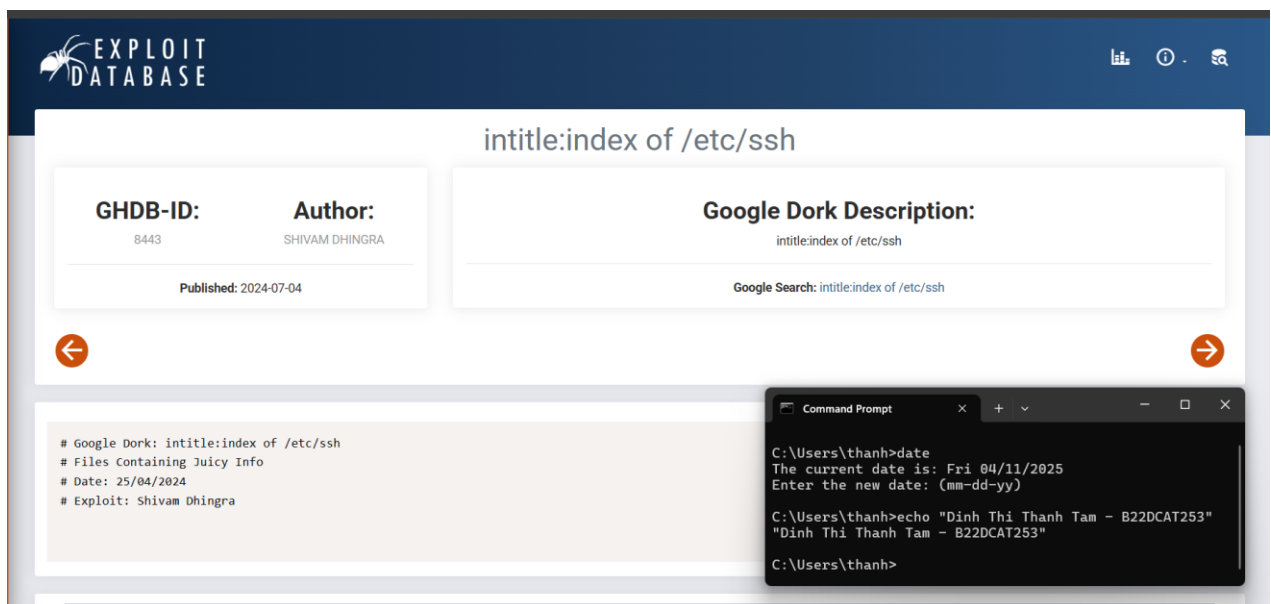
Hình 18 Danh mục Filters

2.1.2.2 Chọn một mục để hiện ra trang thông tin có liên quan bao gồm thông tin tác giả, mô tả về tìm kiếm và các thông tin khác. (ví dụ: Files Containing Passwords)

- Bấm vào danh mục Files Containing Passwords



- Ví dụ chọn dork: `intitle:index of /etc/ssh`
 ➔ Bấm vào kết quả đó, trang chi tiết hiện ra như hình bên dưới:

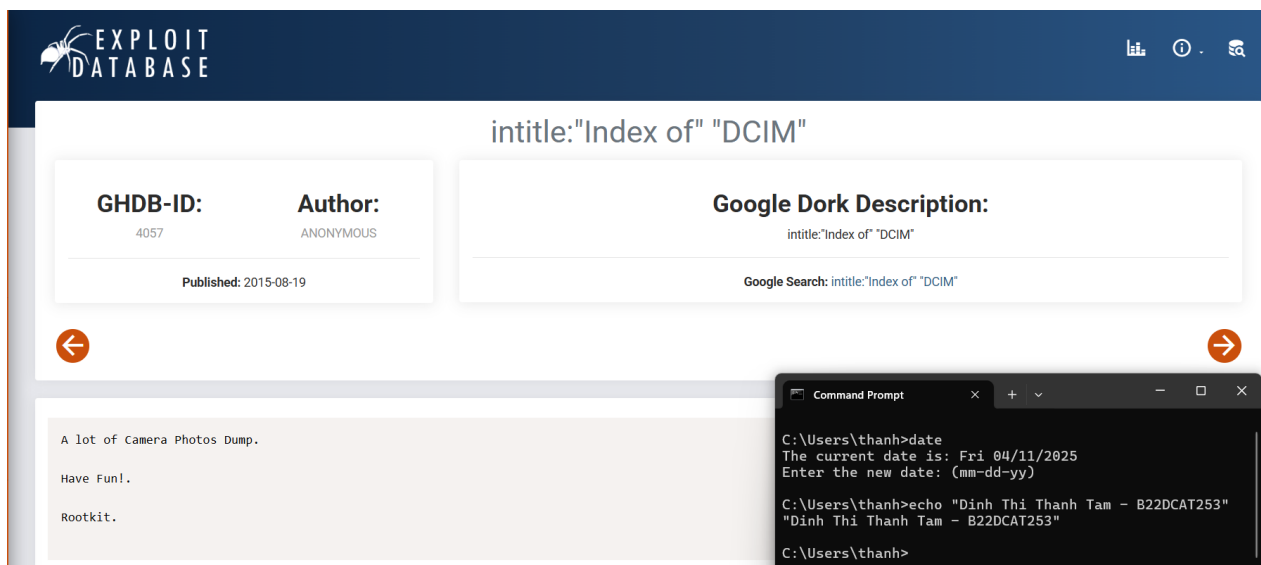


Hình 19 Trang chi tiết dork

- ➔ Trang chi tiết dork sẽ hiển thị:
- Google Dork: `intitle:index of /etc/ssh`
- Tác giả: SHIVAM DHINGRA
- Mô tả: Truy vấn này giúp tìm ra các tệp log chứa thông tin mật khẩu văn bản thường. Những file log như vậy đôi khi được vô tình public trên web.
- Danh mục: Files Containing Passwords
- Nguy cơ: Có thể dẫn đến rò rỉ tài khoản người dùng, email, thông tin đăng nhập...

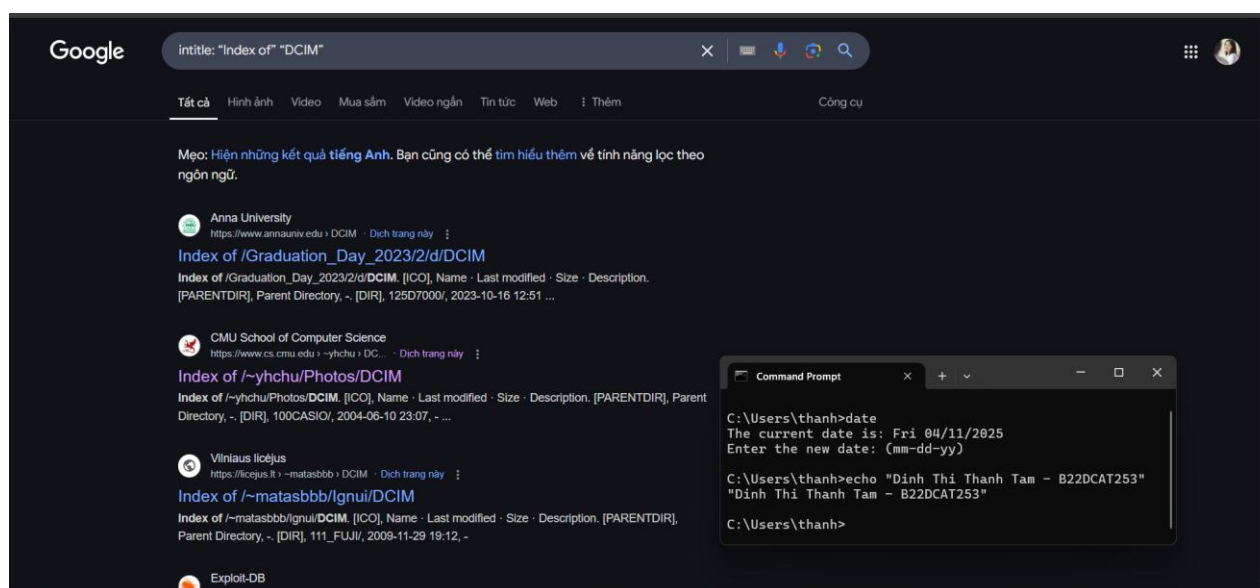
2.1.2.3 Truy cập ví dụ cụ thể

- Truy cập: <https://www.exploit-db.com/ghdb/4057>
- Truy vấn mẫu: `intitle:"Index of" "DCIM"`



Hình 20 Trang chi tiết dork

➔ Dùng Google để tìm thư mục ảnh được public.



Hình 21 Kết quả tìm kiếm bộ sưu tập được công khai bằng Google

- Kết quả nhấp vào siêu liên kết cho các dork thực tế của Google

Index of /~yhchu/Photos/DCIM/100CASIO

Name	Last modified	Size	Description
Parent Directory	-	-	-
CIMG0001.JPG	2002-01-10 11:45	555K	
CIMG0002.JPG	2002-01-12 14:51	537K	
CIMG0003.JPG	2002-01-12 14:52	541K	
CIMG0004.JPG	2002-01-12 14:52	537K	
CIMG0005.JPG	2002-01-12 14:52	556K	
CIMG0006.JPG	2002-01-12 14:53	551K	
CIMG0007.JPG	2002-01-12 14:53	566K	
CIMG0008.JPG	2002-01-12 14:54	543K	
CIMG0009.JPG	2002-01-15 14:18	557K	
CIMG0010.JPG	2002-01-15 14:19	533K	
CIMG0011.JPG	2002-01-15 14:19	526K	
CIMG0012.JPG	2002-01-15 19:11	594K	
CIMG0013.JPG	2002-01-15 19:11	578K	
CIMG0014.JPG	2002-01-15 19:12	593K	
CIMG0015.JPG	2002-01-15 19:13	591K	

```
Command Prompt
C:\Users\thanh>date
The current date is: Fri 04/11/2025
Enter the new date: (mm-dd-yy)

C:\Users\thanh>echo "Dinh Thi Thanh Tam - B22DCAT253"
"Dinh Thi Thanh Tam - B22DCAT253"

C:\Users\thanh>
```

Apache/2.4.18 (Ubuntu) Server at www.cs.cmu.edu Port 443

Hình 22 Kết quả bộ sưu tập ảnh ngẫu nhiên được công khai

➔ Google sẽ trả về kết quả của các bộ sưu tập ảnh mà mọi người không biết ở đó

- Tìm hiểu các từ khóa:
 - intitle: Tìm tiêu đề trang
 - "DCIM": Tên thư mục mặc định chứa ảnh trong camera

2.1.2.4 Google dork tìm các khóa SSH.

- Tìm SSH keys, truy cập:

<https://www.exploit-db.com/ghdb/6322>

exploit-db.com/ghdb/6322

EXPLOIT DATABASE

intitle:"index of" "id_rsa.pub"

GHDB-ID: 6322 **Author:** SID JOSHI

Published: 2020-06-22

Google Dork Description: intitle:"index of" "id_rsa.pub"

Google Search: intitle:"index of" "id_rsa.pub"

Dork: intitle:"index of" "id_rsa.pub"

Author: Sid Joshi

Result of this dorks contains Sensitive Directories with juicy ssh keys.

POC in attachment

Thanks!

```
Command Prompt
C:\Users\thanh>date
The current date is: Fri 04/11/2025
Enter the new date: (mm-dd-yy)

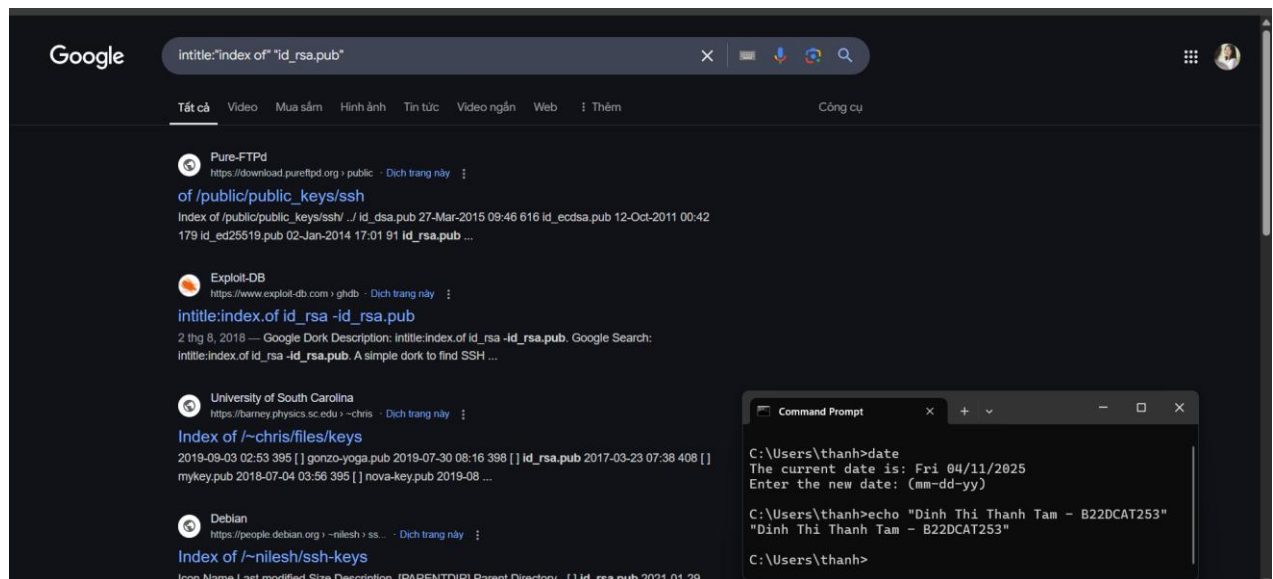
C:\Users\thanh>echo "Dinh Thi Thanh Tam - B22DCAT253"
"Dinh Thi Thanh Tam - B22DCAT253"

C:\Users\thanh>
```

Hình 23 Trang chi tiết dork

➔ Google Dork: `intitle:"index of" "id_rsa.pub"`

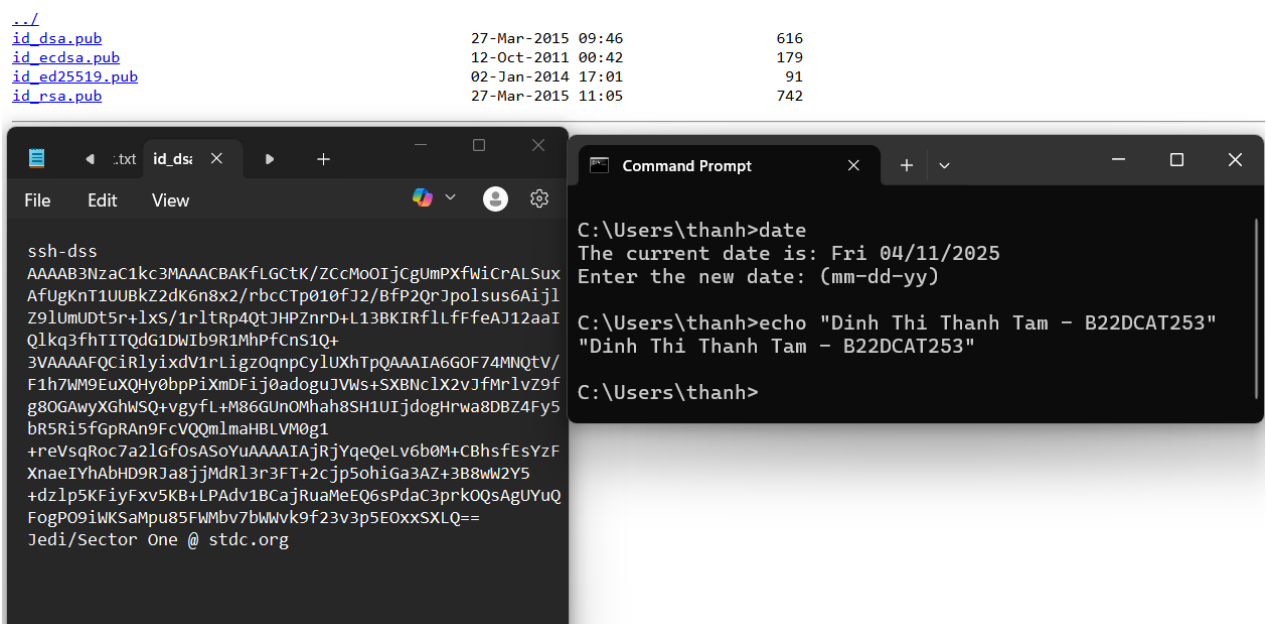
- Dùng Google để tìm tệp tin và thư mục nhạy cảm có chứa khóa ssh:



Hình 24 Kết quả tìm kiếm thư mục chứa khóa ssh được công khai bằng Google

- Kết quả nhấp vào siêu liên kết cho các dork thực tế của Google

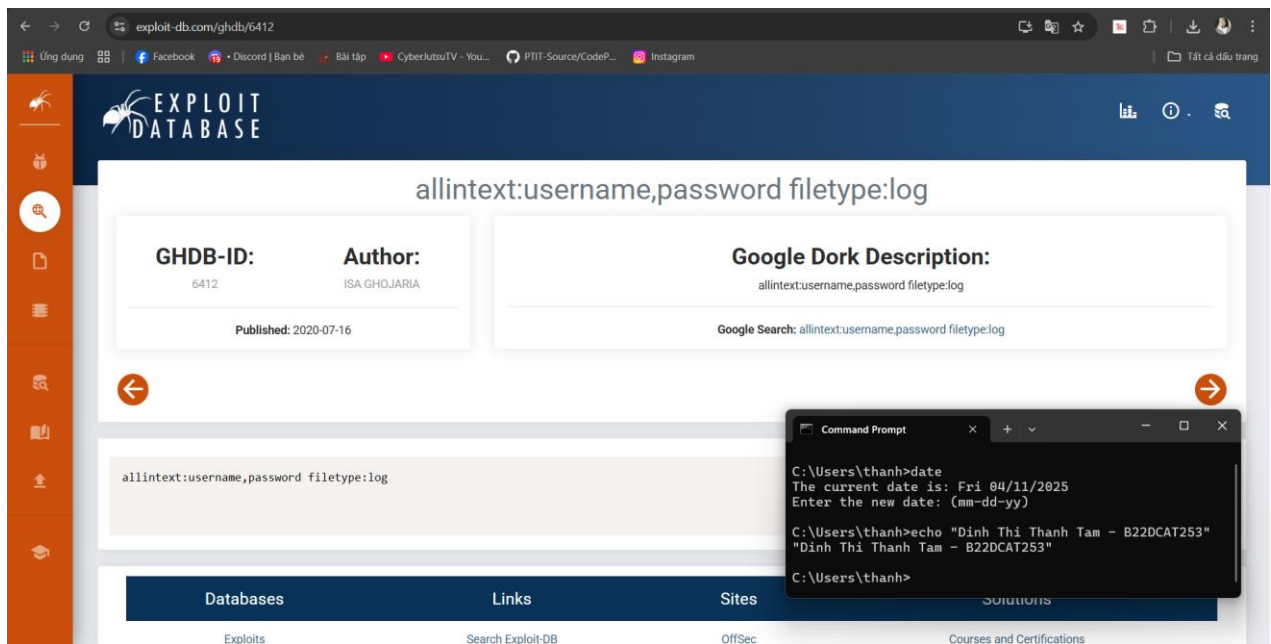
Index of /public/public_keys/ssh/



Hình 25 Kết quả file khóa được công khai ngẫu nhiên

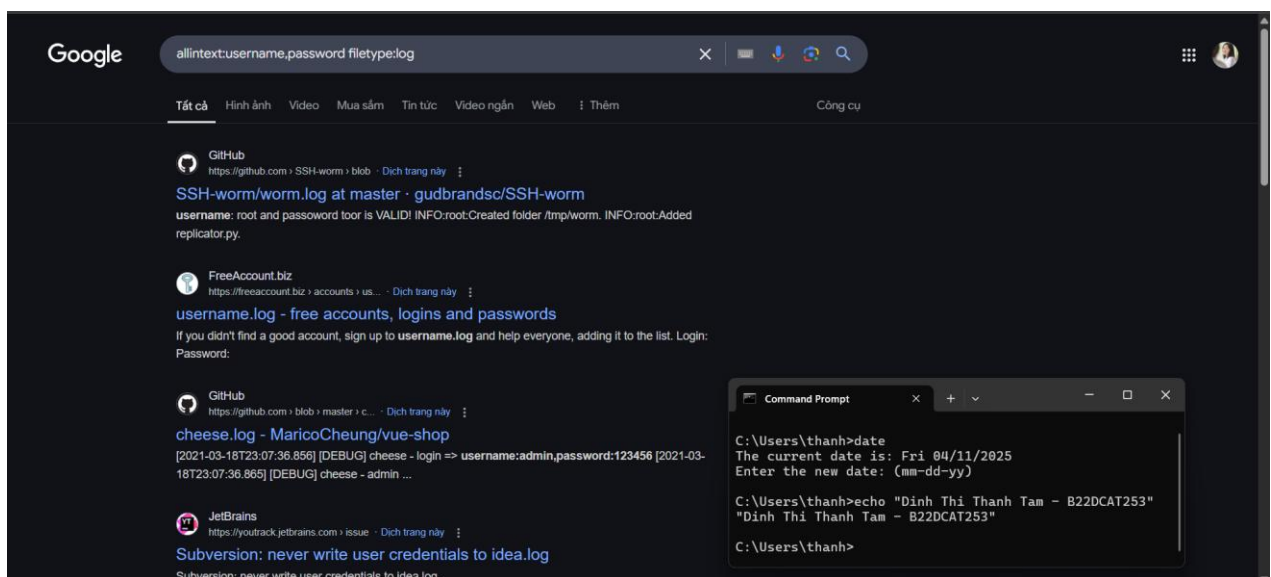
2.1.2.5 Google dork tìm log có tên người dùng và mật khẩu

- Truy cập: <https://www.exploit-db.com/ghdb/6412>



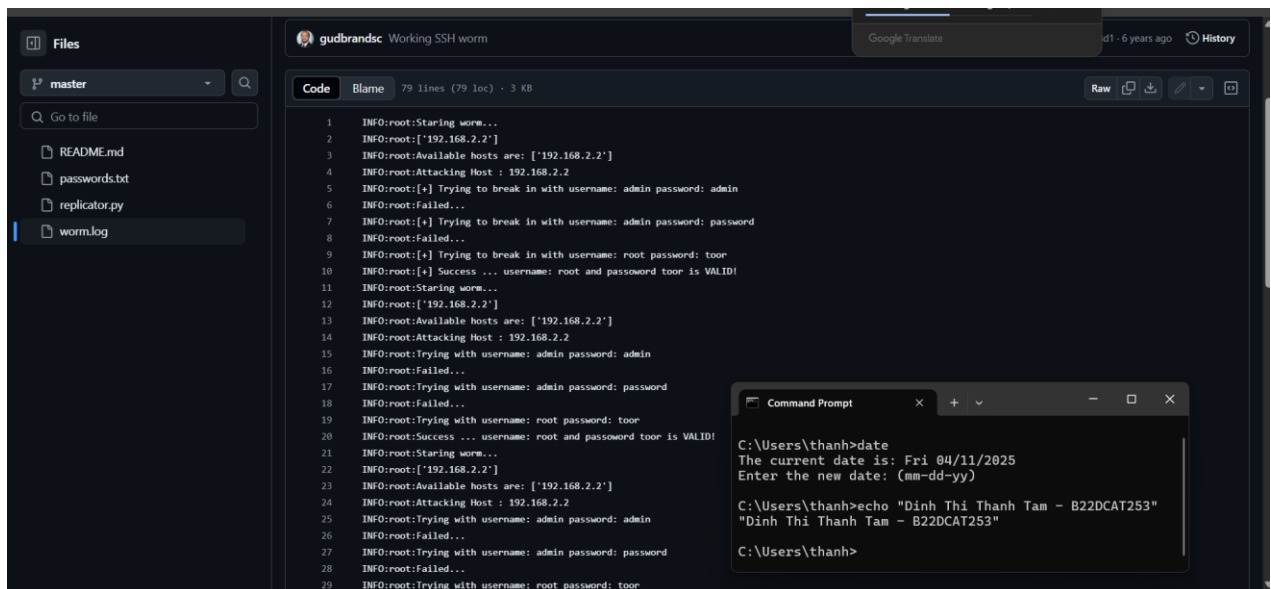
➔ Google dork: allintext:username,password filetype:log

- Dùng Google để tìm log có tên người dùng và mật khẩu:



Hình 26 Kết quả tìm log có tên người dùng và mật khẩu bằng Google

- Kết quả nhấp vào siêu liên kết cho các dork thực tế của Google

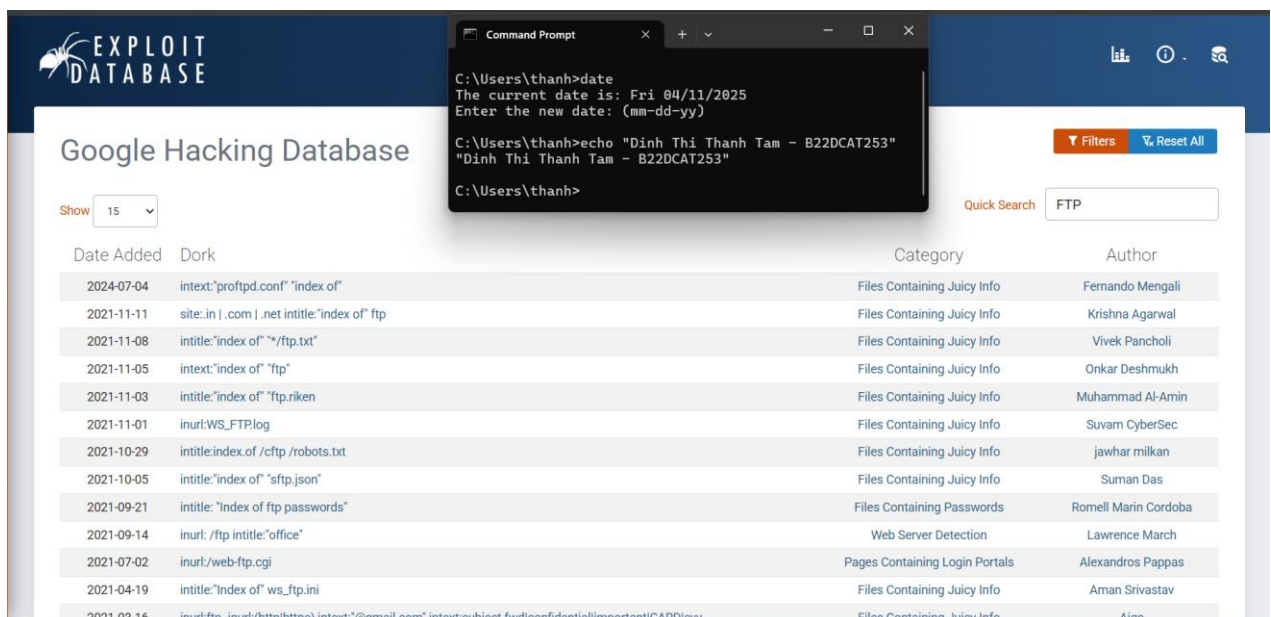


Hình 27 log có tên người dùng và mật khẩu

2.1.2.6 Tìm các dork có liên quan đến FTP

- Vào lại GHDB
- Ở ô “Quick Search” bên phải, nhập:

FTP



Hình 28 Kết quả tìm kiếm “FTP” bằng Quick Search

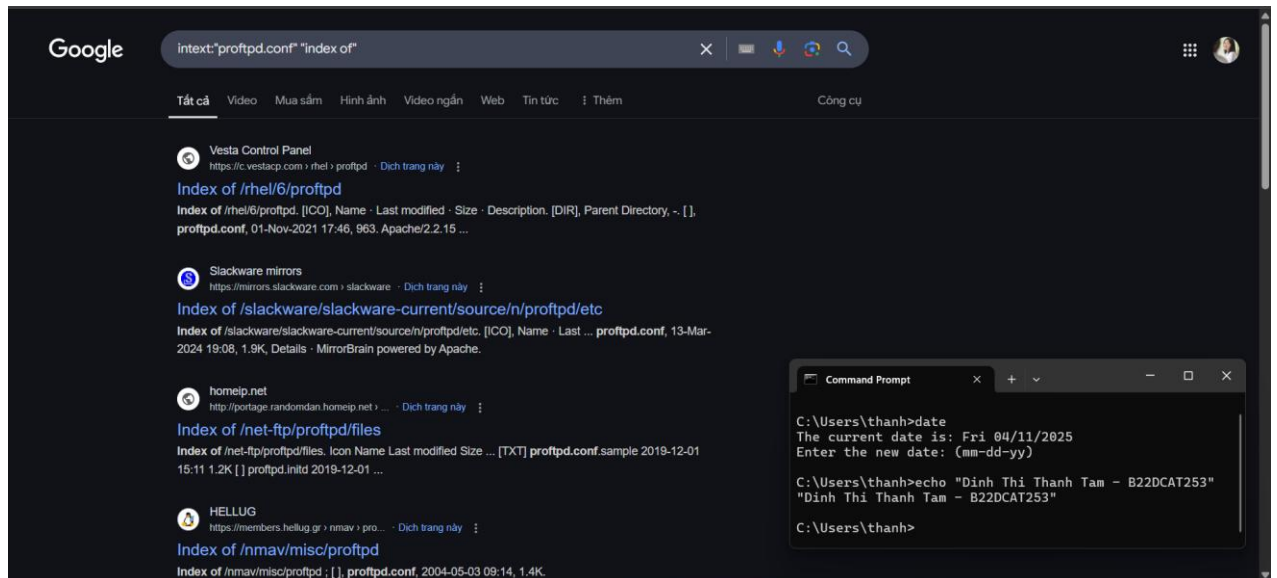
➔ Chọn 5 dork thuộc các loại danh mục khác nhau

1. Chọn dork: intext:"proftpd.conf" "index of"

Thành phần	Ý nghĩa
intext:"proftpd.conf"	Tìm các trang có chứa nội dung là tên file cấu hình ProFTPD
"index of"	Tìm thư mục được liệt kê công khai dưới dạng "Index of" directory listing – tức là thư mục web chưa bị ẩn hoặc bảo vệ

Bảng 3. Giải nghĩa truy vấn intext:"proftpd.conf" "index of"

- Tìm kiếm dork bằng Google



Hình 29 Kết quả tìm kiếm dork bằng Google

- Kết quả nhấp vào siêu liên kết cho các dork thực tế của Google

Index of /net-ftp/proftpd/files

Name	Last modified	Size	Description
Parent Directory	-	-	-
proftpd-1.3.6-use-trace.patch	2019-06-06 19:30	477	
proftpd-1.3.6_rc4-diskuse-refresh-api.patch	2019-06-06 19:30	576	
proftpd-1.3.6_rc4-gss-refresh-api.patch	2019-06-06 19:30	1.8K	
proftpd-1.3.6_rc4-msg-refresh-api.patch	2019-06-06 19:30	903	
proftpd-1.3.6_rc4-vroot-refresh-api.patch	2019-06-06 19:30	736	
proftpd-1.3.8-configure-clang16.patch	2023-05-07 08:55	5.7K	
proftpd-1.3.8a-configure-c99.patch	2023-12-09 18:30	1.0K	
proftpd-tmpfiles.d.conf	2019-06-06 19:30	34	
proftpd-tmpfiles.d.conf-r1	2020-05-30 00:25	30	
proftpd.conf.sample	2019-06-06 19:30	1.2K	
proftpd.initd	2019-06-06 19:30	1.4K	
proftpd.initd-r1	2022-12-04 21:45	1.4K	
proftpd.logrotate	2019-06-15 10:35	237	
proftpd.service	2019-06-06 19:30	196	
proftpd.xinetd	2019-06-06 19:30	295	

Apache/2.4.63 (Gentoo) mod_fcgid/2.3.9 OpenSSL/3.4.1 mod_perl/2.0.13 Perl/v5.40.1 Server at portage.randomdan.homeip.net Port 11080

Hình 30 Kết quả nhấp vào siêu liên kết

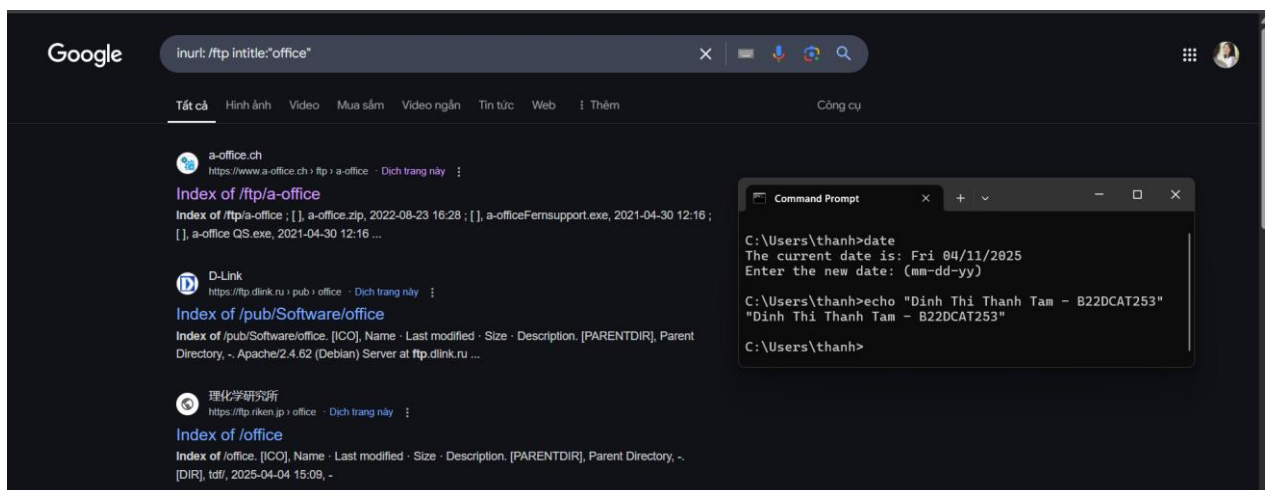
- ➔ Truy vấn `intext:"proftpd.conf" "index of"` giúp xác định các máy chủ web đang công khai thư mục chứa file cấu hình `proftpd.conf`.
- ➔ Nếu bị lộ, attacker có thể thu thập thông tin cấu hình FTP server, từ đó thực hiện các hành vi như dò pass, truy cập ẩn danh, hoặc khai thác lỗ hổng của phần mềm.
- ➔ Truy vấn này cực kỳ nguy hiểm nếu admin không bảo vệ tốt hệ thống thư mục và quyền truy cập file cấu hình.

2. Chọn dork: `inurl: /ftp intitle:"office"`

Thành phần	Ý nghĩa
<code>inurl: /ftp</code>	Tìm các URL có chứa đường dẫn <code>"/ftp"</code> – thường liên quan đến thư mục FTP công khai hoặc dịch vụ FTP chạy qua HTTP
<code>intitle:"office"</code>	Tìm các trang có tiêu đề chứa chữ <code>"office"</code> – gợi ý đây có thể là tài liệu văn phòng, file nội bộ văn phòng hoặc hệ thống văn phòng điện tử

Bảng 4. Giải nghĩa truy vấn `inurl: /ftp intitle:"office"`

- Tìm kiếm dork bằng Google



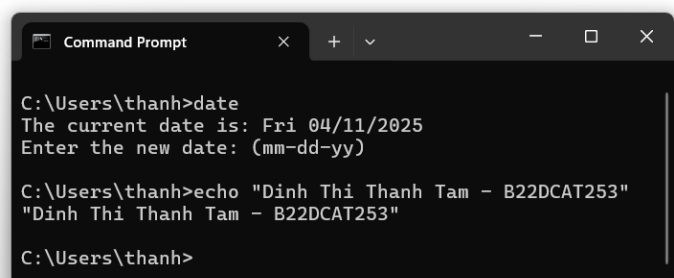
Hình 31 Kết quả tìm kiếm dork bằng Google

- Kết quả nhấp vào siêu liên kết cho các dork thực tế của Google

Index of /ftp/a-office

Name	Last modified	Size	Description
Parent Directory	-	-	-
a-office.zip	2022-08-23 16:28	424M	
a-officeFernsupport.exe	2021-04-30 12:16	1.9M	
a-office.QS.exe	2021-04-30 12:16	14M	
a-office_DEV.zip	2023-03-23 13:33	485M	

Apache Server at www.a-office.ch Port 443

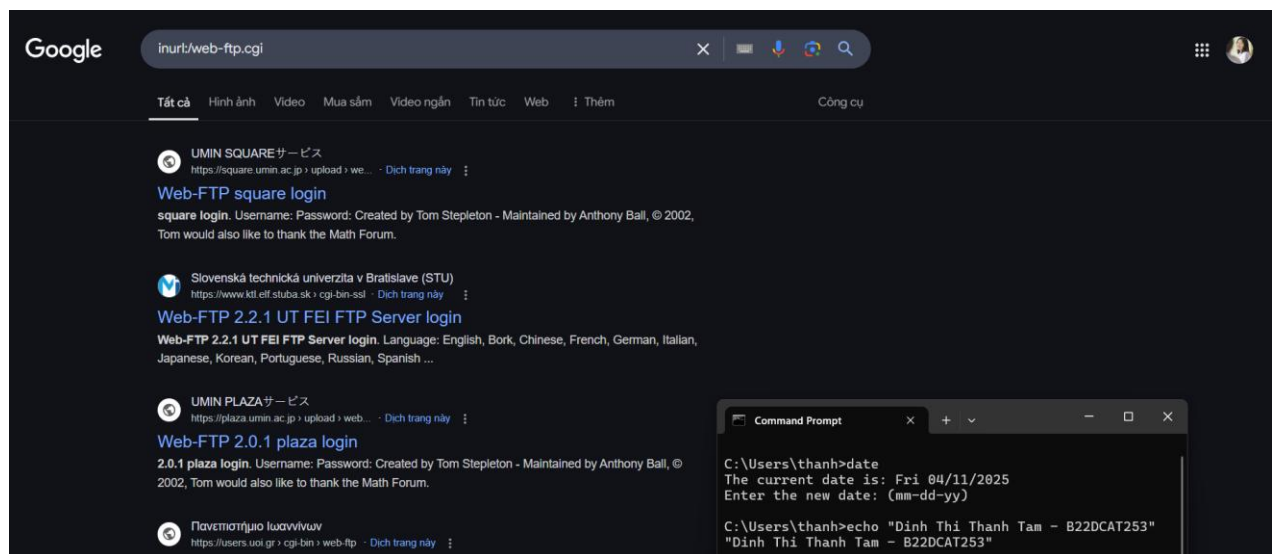


Hình 32 Kết quả nhấp vào siêu liên kết

- ➔ Truy vấn `inurl:/ftp intitle:"office"` nhằm tìm kiếm các thư mục FTP được chia sẻ công khai có liên quan đến tài liệu văn phòng.
- ➔ Đây là truy vấn nguy hiểm vì nó có thể tiết lộ thông tin nhạy cảm như tài liệu nội bộ, hợp đồng, bảng tính tài chính,... của các tổ chức.
- ➔ Việc cấu hình sai hoặc quên bảo mật các thư mục FTP có thể tạo ra rủi ro bảo mật nghiêm trọng.

3. Chọn dork: `inurl:/web-ftp.cgi`

- Giải nghĩa truy vấn: Tìm các URL có chứa đoạn `/web-ftp.cgi` – thường là giao diện web của một trình quản lý FTP trực tuyến (Web FTP Client)
- Tìm kiếm dork bằng Google



Hình 33 Kết quả tìm kiếm dork bằng Google

- Kết quả nhấp vào siêu liên kết cho các dork thực tế của Google

Web-FTP square login

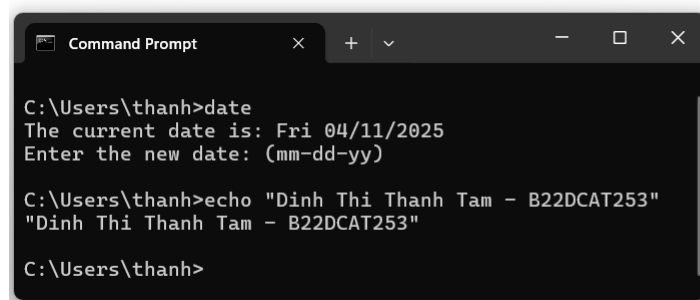
Username:

Password:

login

Created by Tom Stepleton - Maintained by [Anthony Ball](#)

© 2002



Hình 34 Kết quả nhấp vào siêu liên kết

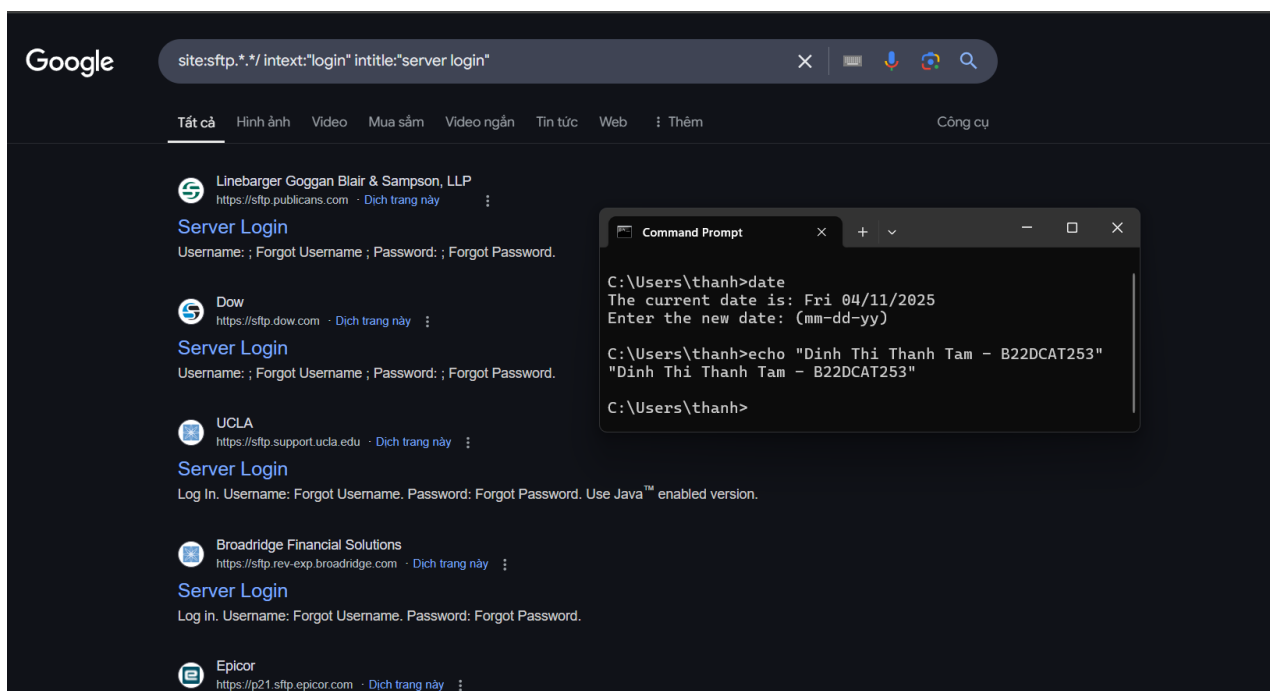
- ➔ Truy vấn `inurl:/web-ftp.cgi` tìm ra các hệ thống đang sử dụng trình duyệt FTP thông qua giao diện web CGI.
- ➔ Nếu hệ thống này không được bảo mật đầy đủ, kẻ tấn công có thể truy cập trái phép vào máy chủ FTP hoặc khai thác các lỗ hổng như RCE hoặc LFI.
- ➔ Đây là một truy vấn tiềm ẩn nguy cơ cao, đặc biệt khi phiên bản `web-ftp.cgi` đã cũ hoặc cấu hình sai.

4. Chọn dork: `site:sftp.*.*/ intext:"login" intitle:"server login"`

Thành phần	Ý nghĩa
<code>site:sftp.*.*/</code>	Tìm các tên miền con hoặc máy chủ sử dụng giao thức SFTP (SSH File Transfer Protocol) – gợi ý đây là hệ thống truyền file an toàn
<code>intext:"login"</code>	Tìm các trang có chứa chữ “login” trong nội dung – tức là có giao diện đăng nhập
<code>intitle:"server login"</code>	Tìm các trang có tiêu đề là “server login” – thường là portal quản trị hoặc giao diện đăng nhập vào máy chủ từ xa

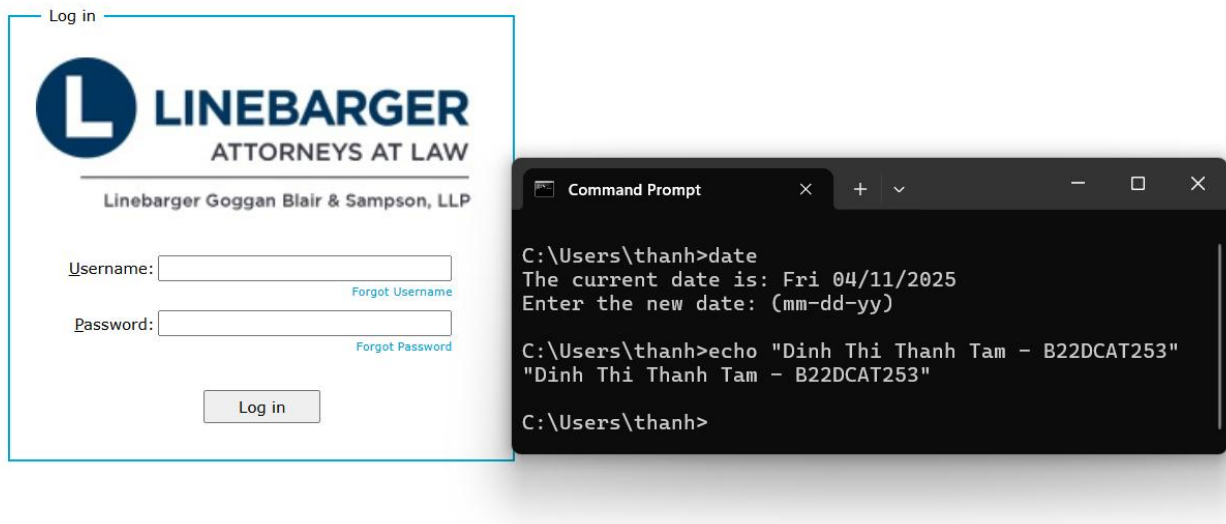
Bảng 5. Giải nghĩa truy vấn `site:sftp..*/ intext:"login" intitle:"server login"`*

- Tìm kiếm dork bằng Google



Hình 35 Kết quả tìm kiếm dork bằng Google

- Kết quả nhấp vào siêu liên kết cho các dork thực tế của Google



Hình 36 Kết quả nhấp vào siêu liên kết

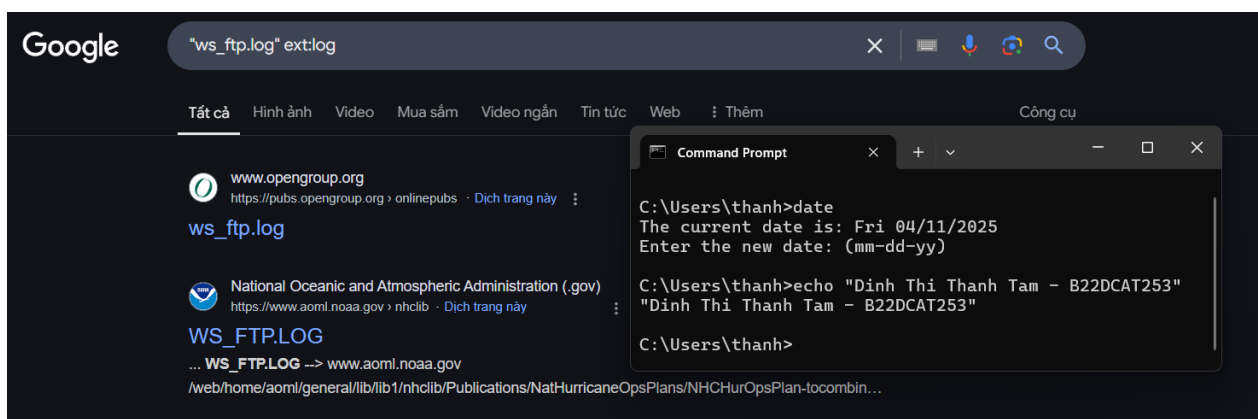
- ➔ Truy vấn site:sftp.*.*/ intext:"login" intitle:"server login" nhằm tìm kiếm các cổng đăng nhập SFTP công khai trên Internet.
- ➔ Đây là một truy vấn nguy hiểm vì nó giúp kẻ tấn công định vị chính xác các giao diện quản lý máy chủ từ xa thông qua giao thức SFTP.
- ➔ Nếu các hệ thống này bị cấu hình sai hoặc không có giới hạn đăng nhập, kẻ tấn công có thể thử brute-force để chiếm quyền truy cập

5. Chọn dork: "ws_ftp.log" ext:log

Thành phần	Ý nghĩa
"ws_ftp.log"	Tìm file log có tên "ws_ftp.log" – đây là log mặc định của phần mềm WS_FTP
ext:log	Chỉ tìm những file có đuôi .log, thường là file nhật ký (log file) ghi lại quá trình kết nối, truy cập, lỗi hệ thống...

Bảng 6. Giải nghĩa truy vấn "ws_ftp.log" ext:log

- Tìm kiếm dork bằng Google



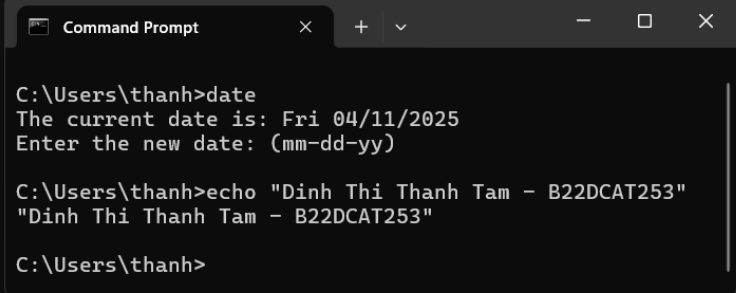
Hình 37 Kết quả tìm kiếm dork bằng Google

- Kết quả nhập vào siêu liên kết cho các dork thực tế của Google

```

103.01.23 21:37 B C:\Tmp\LDAP\I031\chap01.htm --> xoneweb.rdg.opengroup.org /web/top/products/publications/pending/I031 chap01.htm
103.01.23 21:37 B C:\Tmp\LDAP\I031\chap02.htm --> xoneweb.rdg.opengroup.org /web/top/products/publications/pending/I031 chap02.htm
103.01.23 21:37 B C:\Tmp\LDAP\I031\chap03.htm --> xoneweb.rdg.opengroup.org /web/top/products/publications/pending/I031 chap03.htm
103.01.23 21:37 B C:\Tmp\LDAP\I031\chap04.htm --> xoneweb.rdg.opengroup.org /web/top/products/publications/pending/I031 chap04.htm
103.01.23 21:37 B C:\Tmp\LDAP\I031\docix.htm --> xoneweb.rdg.opengroup.org /web/top/products/publications/pending/I031 docix.htm
103.01.23 21:37 B C:\Tmp\LDAP\I031\front.htm --> xoneweb.rdg.opengroup.org /web/top/products/publications/pending/I031 front.htm
103.01.23 21:37 B C:\Tmp\LDAP\I031\toc.htm --> xoneweb.rdg.opengroup.org /web/top/products/publications/pending/I031 toc.htm
103.01.23 21:38 B C:\Tmp\LDAP\i031\chap01.htm --> xoneweb.rdg.opengroup.org /web/top/products/publications/pending/i031 chap01.htm
103.01.23 21:38 B C:\Tmp\LDAP\i031\chap02.htm --> xoneweb.rdg.opengroup.org /web/top/products/publications/pending/i031 chap02.htm
103.01.23 21:38 B C:\Tmp\LDAP\i031\chap03.htm --> xoneweb.rdg.opengroup.org /web/top/products/publications/pending/i031 chap03.htm
103.01.23 21:38 B C:\Tmp\LDAP\i031\chap04.htm --> xoneweb.rdg.opengroup.org /web/top/products/publications/pending/i031 chap04.htm
103.01.23 21:38 B C:\Tmp\LDAP\i031\docix.htm --> xoneweb.rdg.opengroup.org /web/top/products/publications/pending/i031 docix.htm
103.01.23 21:38 B C:\Tmp\LDAP\i031\front.htm --> xoneweb.rdg.opengroup.org /web/top/products/publications/pending/i031 front.htm
103.01.23 21:38 B C:\Tmp\LDAP\i031\toc.htm --> xoneweb.rdg.opengroup.org /web/top/products/publications/pending/i031 toc.htm

```



```

C:\Users\thanh>date
The current date is: Fri 04/11/2025
Enter the new date: (mm-dd-yy)

C:\Users\thanh>echo "Đinh Thi Thanh Tam - B22DCAT253"
"Đinh Thi Thanh Tam - B22DCAT253"

C:\Users\thanh>

```

Hình 38 Kết quả nhập vào siêu liên kết

- ➔ Truy vấn “ws_ftp.log” ext:log tìm kiếm các file nhật ký FTP được tạo bởi phần mềm WS_FTP.
- ➔ Đây là file nhạy cảm vì nó có thể chứa thông tin đăng nhập, IP truy cập, và cấu trúc hệ thống. Nếu bị lộ, kẻ tấn công có thể khai thác để dò mật khẩu, truy cập trái phép hoặc lên kế hoạch tấn công vào hệ thống.
- ➔ Truy vấn này đặc biệt nguy hiểm nếu quản trị viên quên xóa file log sau khi sử dụng.

KẾT LUẬN

- Lý thuyết về Shodan, Google Hacking
- Thử nghiệm thành công 10 ví dụ tìm kiếm trong shodan để tìm kiếm các lỗ hổng, các thiết bị hay dịch vụ, sử dụng các bộ lọc đã tìm hiểu bên trên.
- Thử nghiệm thành công 10 ví dụ Google hacking như đã tìm hiểu bên trên.

TÀI LIỆU THAM KHẢO

- [1] <https://www.yeahhub.com/find-vulnerable-webcams-shodan-metasploit-framework/>
- [2] <https://money.cnn.com/gallery/technology/security/2013/05/01/shodan-most-dangerous-internet-searches/index.html>
- [3] Principles of Computer Security: CompTIA Security+ and Beyond